PROPOSAL FOR TOPIC APPROVAL TO BE SUBMITTED TO THE UNIVERSITY OF MUMBAI FOR THE DEGREE OF **Ph.D. (SCIENCE AND TECHNOLOGY)** IN THE SUBJECT OF **INFORMATION TECHNOLOGY**

Title of Topic	:	Enhancing Smart Web Access Using Honeywords, Keystroke Dynamics and Fuzzy Logic Membership Functions
Name of the Student	:	Mr. Siddhesh Ashok Vaidya
Basic Qualification	:	M.E.(Information Technology) B.E.(Information Technology)
In the Case of Ph.D. student Year of Passing of PET/NET/SET/GATE (Teaching Experience)	:	PET - 2021 (75/100)
Name of the Research Supervisor/ Guide	:	Dr. Bhavesh Valji Patel
Date of Superannuation/ Retirement	:	20/03/2036
Name of the Research Center	:	Shah and Anchor Kutchhi Engineering College
Signature of Student	:	
Signatue of the Research Supervisor	:	

Shah & Anchor Kutchhi Engg. College Autonomous Institute Mumbai-88

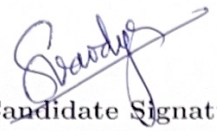
Head / Director / Principal
Research Centre

Dr. Bhavesh Patel
Principal
Shah & Anchor Kutchhi Engg. College
Waman Tukaram Patil Marg,
Next to Dukes Co., Chembur,
Mumbai - 400 088.

Sr. No.	Content	Page No.
1	Introduction	1
2	Research Hypothesis	4
3	Aim & Objectives	6
4	Materials & Methods	7
5	Expected Results/Outcomes	8
6	References	9

Statement by the Candidate

I wish to state that the work embodied in this synopsis titled "Enhancing Smart Web Access Using Honeywords, Keystroke Dynamics and Fuzzy Logic Membership Functions" forms my own contribution to the work carried out under the guidance of Dr. Bhavesh Valji Patel at the Shah and Anchor Kutchhi Engineering College. I declare that this written submission represents my ideas in my own words and where others ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.



(Candidate Signature)

Name: Mr. Siddhesh Vaidya

Roll Number: 23DF18605IT002

Introduction

In the realm of cybersecurity, detecting unauthorized access attempts and safeguarding sensitive information are critical challenges. Traditional methods such as password protection and straight forward authentication techniques, while foundational, are often insufficient on their own. To bolster security, a multifaceted approach incorporating Honeywords, Keystroke Dynamics, and Fuzzy Logic Membership Functions can be employed [1].

Honeywords are decoy passwords that are designed to mislead attackers and detect unauthorized access attempts [6] - [10]. When an intruder tries to use a honeyword, it triggers an alert, allowing for immediate detection of a potential breach. This technique adds a layer of deception, where real passwords are mixed with fake ones to enhance the security of authentication systems [15]. The honeywords are strategically chosen to mimic real passwords, making it difficult for attackers to differentiate between genuine and fake credentials [9].

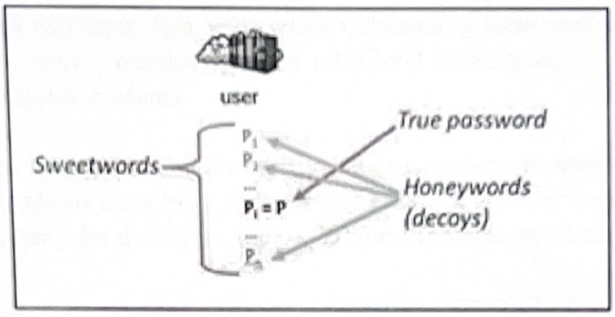


Figure 1: Honeywords

Keystroke dynamics involves analyzing the unique patterns of how individuals type on a keyboard [30] - [31]. This biometric method captures and evaluates the timing and rhythm of keystrokes, including factors such as the duration of key presses and the speed between keystrokes. By establishing a baseline profile for legitimate users, the system can detect deviations that may indicate unauthorized access. For instance, if an attacker attempts to impersonate a user, their typing patterns will likely differ from those of the legitimate user, triggering suspicion [18].

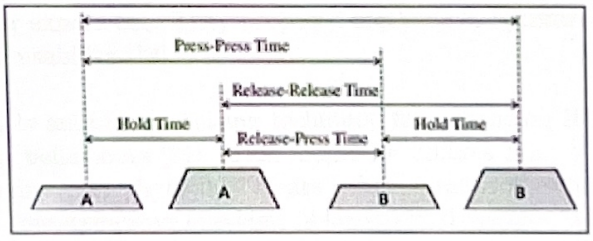


Figure 2: Keystroke Dynamics

Fuzzy logic introduces a flexible approach to handle uncertainty and imprecision in data. In the context of intrusion detection, fuzzy logic membership functions [2] can be employed to evaluate and interpret the data from honeywords and keystroke dynamics. These functions allow for the assessment

of degrees of membership, meaning that rather than making a binary decision, the system can handle varying levels of confidence regarding the authenticity of the user. By incorporating fuzzy logic, the system can provide a more nuanced evaluation of the risk of intrusion, accommodating uncertainties and variances in user behaviour. Another name for fuzzy logic is "Fuzzy Reasoning". This term highlights the aspect of reasoning under uncertainty and imprecision, which is central to fuzzy logic's approach to handling complex and vague information.

Combining honeywords, keystroke dynamics, and fuzzy logic enhances the robustness of intrusion detection systems [13]. Honeywords create a deceptive layer that confuses potential attackers [11] - [12], keystroke dynamics add a behavioral biometric check, and fuzzy logic provides a sophisticated method for interpreting the collected data [16]. Together, these technologies form a comprehensive defense mechanism that not only detects potential breaches but also adapts to the evolving nature of cyber threats [17].

This integrated approach offers a more resilient and intelligent security framework, capable of addressing a wide range of intrusion scenarios while minimizing false positives and negatives [5]. As cyber threats continue to evolve, employing such advanced techniques is crucial in maintaining the integrity and security of digital systems.

Such Systems are vital for identifying and mitigating unauthorized access and threats within computer systems. Various methods have been proposed to enhance these systems' effectiveness, including the use of honeywords, keystroke dynamics [28] - [29], and fuzzy logic membership functions.

Honeywords represent a novel approach to improving password security [3]. The concept involves embedding fake passwords, or honeywords, alongside genuine ones in a password database [4]. These honeywords serve as decoys, triggering alerts when an attacker attempts to access or crack the database [7]. Schechter et al. (2014) pioneered this idea, demonstrating how honeywords could substantially increase the difficulty of password cracking and improve overall security by making it less straightforward for attackers to distinguish between real and fake passwords [8]. Building on this foundation, Dagon et al. (2016) proposed practical strategies for implementing honeywords and assessed their effectiveness against various types of attacks, including those that involve brute-force or dictionary attacks. Their work highlighted how honeywords could be effectively integrated into existing systems without significantly compromising user convenience. Gupta et al. (2017) addressed challenges in deploying honeywords, such as the need to balance the number of honeywords with system performance and user experience. They proposed methods to optimize honeyword deployment to ensure both security and usability [14].

Keystroke Dynamics is another promising technique for enhancing IDS by analyzing the unique patterns in users' typing behaviours [21]. This method evaluates aspects such as typing speed, key press intervals, and overall typing rhythm to create behavioural profiles for users [22] - [23]. Law and Chan (2005) provided a comprehensive overview of keystroke dynamics, discussing various algorithms and their effectiveness in authenticating users and detecting anomalies. They highlighted that while keystroke dynamics offers a promising supplementary authentication method, its performance can vary based on individual typing patterns and environmental factors. Liu et al. (2012) conducted a survey comparing keystroke dynamics with other biometric systems, emphasizing its advantages in terms of unobtrusiveness and the ability to capture behavioural traits that are difficult to mimic. Johnston and Smith (2018) further advanced the field by incorporating temporal data into keystroke dynamics

analysis, which improved the accuracy and reliability of user authentication systems. Their approach demonstrated that integrating additional data could enhance the robustness of keystroke dynamics in detecting fraudulent behavior [19] - [20].

Fuzzy logic provides a valuable framework for managing uncertainty and imprecision in IDS. By employing fuzzy logic membership functions, systems can assess inputs in a way that reflects the inherent ambiguity of real-world data. Nguyen and Islam (2011) reviewed the application of fuzzy logic in IDS, highlighting how membership functions can be used to model complex and uncertain threat scenarios. They noted that fuzzy logic allows for more flexible and nuanced decision-making compared to traditional binary systems. Al-Ali et al. (2015) proposed a hybrid IDS approach combining fuzzy logic with other techniques, such as statistical methods and machine learning algorithms, to improve overall detection capabilities. Their work demonstrated that fuzzy logic could effectively handle the variability and complexity of intrusion patterns, enhancing the systems ability to detect and respond to sophisticated attacks. Sundararajan and Prakash (2020) provided a detailed survey of fuzzy logic-based IDS, comparing different membership functions and their performance in various intrusion scenarios. They discussed how fuzzy logic could be tailored to specific security needs and threat environments, highlighting its adaptability and effectiveness.

Recent research has increasingly focused on integrating these methods to create more comprehensive and robust IDS. For instance, combining honeywords with keystroke dynamics could provide an additional layer of security, where the presence of honeywords might be used to validate the authenticity of keystroke patterns [24] - [25]. Fuzzy logic could then be employed to analyze the combined data, offering a more nuanced assessment of potential threats. This integrated approach promises to enhance intrusion detection by leveraging the strengths of each technique while addressing their individual limitations. Future research is likely to continue exploring these integrations, aiming to develop adaptive and practical systems that can effectively respond to evolving cybersecurity challenges.

This detailed exploration of honeywords, keystroke dynamics [26] - [27], and fuzzy logic membership functions underscores the innovative approaches being applied to improve intrusion detection systems. As these techniques evolve and become more sophisticated, they offer promising avenues for enhancing security and protecting against increasingly sophisticated threats.

Research Hypothesis

Incorporating fuzzy logic membership functions into the analysis of keystroke dynamics alongside honeywords improves the accuracy of distinguishing between genuine and fraudulent authentication attempts, leading to a more robust security mechanism.

Fuzzy Logic: This approach involves many-valued logic, dealing with approximate reasoning instead of precise values. Applied to keystroke dynamics, fuzzy logic accommodates variations and uncertainties in typing patterns, allowing for a more nuanced evaluation of authentication attempts.

Honeywords: These are fake passwords designed to identify unauthorized access. Incorporating fuzzy logic enables the system to manage the uncertainties and variations in typing these honeywords more effectively.

Keystroke Dynamics: This technique analyses typing patterns, including speed. Fuzzy logic can handle natural variations in a user's typing behaviour, as well as the subtle differences that occur when typing honeywords.

Components of the Hypothesis

1. Fuzzy Logic Membership Functions: Implement fuzzy logic to evaluate keystroke dynamics by defining membership functions for typing characteristics (e.g. typing speed, dwell time, flight time). This will allow the system to assess how close an input is to the legitimate users pattern in a probabilistic manner rather than a binary decision.

2. Enhanced Detection Accuracy: Use fuzzy logic to differentiate between real and honeyword passwords by evaluating the fuzzy membership values of the typing patterns. This approach should improve the accuracy of identifying fraudulent attempts even when attackers use sophisticated techniques to mimic typing patterns.

3. Improved Security and Usability: The hypothesis suggests that this method will not only enhance security by reducing false positives and false negatives (FAR and FRR), but will also maintain or improve user experience by accommodating natural typing variations.

Study Design

1. Define Membership Functions: Develop fuzzy logic membership functions for key keystroke dynamics parameters, such as:

i. Dwell Time: The duration a key is held down.

ii. Flight Time: The time between releasing one key and pressing the next.

iii. Typing Speed: The overall speed of typing.

2. Create a Test Database: Build a database with real passwords, honeywords, and corresponding keystroke dynamics profiles, include variations in typing patterns for both legitimate users and

attackers.

3. Simulate Authentication Scenarios: Conduct authentication trials where users type real passwords, honeywords, and simulated fraudulent attempts. Record keystroke dynamics for each case.

4. Apply Fuzzy Logic Analysis: Use the defined fuzzy membership functions to analyze the keystroke dynamics. Determine the degree to which each input matches the expected pattern for real versus honeyword passwords.

5. Evaluate Performance: Measure the performance of the system in terms of:
i. Accuracy: How well it distinguishes between genuine and fraudulent attempts.
ii. False Acceptance Rate (FAR) The rate at which fraudulent attempts are incorrectly accepted.
iii. False Rejection Rate: The rate at which legitimate attempts are incorrectly rejected.

6. User Experience: Assess the impact on user experience, focusing on login speed and ease of use.

Aims & Objectives

The proposed research aims to built an application which enhances security level a step ahead by considering factors such as combination of original as well as fake credentials, variations in users typing pattern (Keystroke Dynamics) with the help of Fuzzy logic membership functions and produce efficiency in terms of FAR and FRR.

- Generation of Honeywords using CHAT GPT API and dictionary algorithm.
- Authenticating users using Fuzzy Logic Membership Functions.
- Generating behavioural paterns of users.
- Authentication using honeywords.
- Security efficiency calculation and studying different algorithms.

Materials & Methods

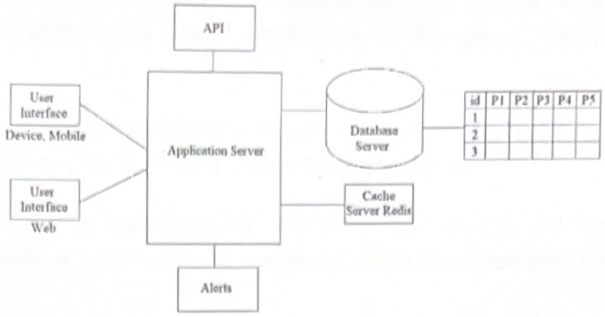


Figure 3: Block Diagram

User Interface: User can interact with the application through Web or handheld devices.

Cache Server Redis: Redis stores data in memory, making it incredibly fast for read and write operations compared to disk-based storage systems.

Application Server: User interacts with the application server which then further communicates with database server to verify original passwords and the Honeywords.

Honeyword Service: Stores hash password in database table at some random generated column number or index and it also stores the actual password index in Redis cache. Additionally, it generates hashed Honeywords h1, h2, , hn and stores in same table where password resides but in different columns.

Honeyword Generation: We will use combination of Chat GPT API and dictionary algorithm to generate similar words/Honeywords.

Fuzzylogic Membership Functions: Fuzzy logic is a form of many-valued logic that deals with approximate reasoning rather than fixed and exact. Membership functions are a key component of fuzzy logic systems. They define how each point in the input space is mapped to a membership value between 0 and 1.

Alerts: During authentication, passwords entered by user will be compared with Honeywords and it will be also verified against the index. If wrong password or authentication failed due to Honeywords or authentication using Fuzzy Logic, alerts will be sent to the user to block the account and if user is not responding, the system will block user account after third failure attempt.

Expected Results/Outcomes

- **Improved Distinction:** Fuzzy logic should enhance the system's ability to distinguish between real and honeyword passwords based on keystroke dynamics, reducing the risk of successful attacks.
- **Adaptability:** The system should handle natural variations in typing patterns more effectively, leading to better user experience and fewer false rejections.
- **Increased Security:** The combination of honeywords and fuzzy logic-enhanced keystroke dynamics should provide a more secure authentication mechanism, making it more difficult for attackers to bypass.

References

[1] M. Sridhar, T. Abraham, J. Rebello, W. Dsouza, and A. DSouza, "Intrusion Detection Using Keystroke Dynamics", Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing, 2013, Springer, pp. 137 - 144.

[2] M. Sridhar, S. Vaidya, and P. Yawalkar, "Intrusion Detection Using Keystroke Dynamics Fuzzy Logic Membership Functions", 2015 International Conference on Technologies for Sustainable Development (ICTSD), Mumbai.

[3] A. Juels and R. L. Rivest, "Honeywords: Making Password-Cracking Detectable", ACM Digital Library, Germany, 2013, pp. 145 - 159.

[4] N. Chakraborty, Y. Yamout, and M. Zulkernine, "The Tables Have Turned: GPT 3 Distinguishing Passwords from Honeywords", 2023 IEEE Conference on Communications and Network Security (CNS), USA.

[5] I. Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords", IEEE Transactions on Dependable and Secure Computing (Vol: 13, No: 2, 01 Mar. 2016), pp. 284 295.

[6] K. Akshaya, and S. Dhanabal, "Achieving Flatness from Non-Realistic Honeywords", 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2017.

[7] S. S. Lingutla, M. V. Nety, and M. V. Martin, "Beyond Chunking: Re-Engineering Password Segmentation for Better Honeywords", 2023 11th International Conference in Software Engineering Research and Innovation (CONISOFT), 2023, IEEE Computer Society Digital Library, pp. 92 - 98.

[8] Akshima, D. Chang, A. Goel, S. Mishra, and S. K. Sanadhya, "Generation of Secure and Reliable Honeywords, Preventing False Detection", IEEE Transactions on Dependable and Secure Computing, (Vol: 16, No: 5, 01 Sep. 2019), pp. 757 - 769.

[9] M. Vydelingum, and M. V. Martin, "How Password Strength Becomes a Weak Link for Honeywords", 2023 11th International Conference in Software Engineering Research and Innovation (CONISOFT), 2023, IEEE Computer Society Digital Library, pp. 99 - 107.

[10] D. Wang, Y. Zou, Q. Dong, Y. Song, and X. Huang, "How to Attack and Generate Honeywords", 2022 IEEE Symposium on Security and Privacy (SP), San Francisco.

[11] J. Brindtha, K. R. Hithaeishini, R. Komala, G. Abirami, U. Arul, "Identification and detecting of attacker in a purchase portal using honeywords", 2017 Third International Conference on Science Technology Engineering Management (ICONSTEM), Chennai.

[12] S. Thakur, S. Chaudhari, and B. Joshi, "Malicious User Detection using Honeywords", 2023 International Conference on Communication System, Computing and IT Applications (CSCITA), Mumbai.

[13] F. Heryanto, S. Siswantyo, and A. S. Widyanti, "Modification of LAKA Protocol Using Fuzzy Verifier and Honeywords", 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), Indonesia.

[14] N. Chakraborty, M. Shojafar, Z. Chen, C. M. Leung, J. Li, and M. Zulkernine, "NESec: A Modified-UI Honeyword Generation Strategy for Mitigating Targeted Guessing Attacks", 2023 7th Cyber Security in Networking Conference (CSNet), Canada.

[15] M. A. Fauzi, B. Yang, and E. Martiri, "PassGAN Based Honeywords System", 2019 International Conference on Computational Science and Computational Intelligence (CSCI), USA.

[16] V. R. Pagar and R. G. Pise, "Strengthening Password Security through Honeyword and HoneyEncrytion Technique", 2017 International Conference on Trends in Electronics and Informatics (ICEI), Tiruvelneli.

[17] A. Banik, A. Das, and A. Dey, "Toward Developing a Password Breach Detection Technique for Serving the Purpose of Honeywords", 2022 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Raipur.

[18] N. Bussabong and T. Anusas-amornku, "Enhanced Keystroke Dynamics Authentication Using Keystroke Vector Dissimilarity", 2023 15th International Conference on Information Technology and Electrical Engineering (ICITEE), Thailand, pp. 223 - 228.

[19] B. Tural, Z. rpek, and S. zmen, "Artificial Intelligence and Keystroke Dynamics: The Mysterious World of Personal Signatures", 2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Turkey.

[20] P. Vaishnav, L.Raja, and Aniket Bhange, "Three layered Multimodal Biometric Authentication on Smartphone using Keystroke Dynamics and Touch Dynamics", 2023 IEEE International Conference on Contemporary Computing and Communications (InC4), Bangalore.

[21] J. Sabu, Ananthanarayanan S, A. Gopan, Gowtham S, and Shalu Murali, "Advanced Keylogger with Keystroke Dynamics", 2023 International Conference on Inventive Computation Technologies (ICICT), Nepal.

[22] R. Chandok, V. Bhoir, and S. Chinnaswamy, "Behavioural Biometric Authentication using Keystroke Features with Machine Learning", 2022 IEEE 19th India Council International Conference (INDICON), Kochi.

[23] N. Gonzlez; E. P. Calot; J. Ierache; W. Hasperu, "The Reverse Problem of Keystroke Dynamics: Guessing Typed Text with Keystroke Timings Only", 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), South Africa.

[24] A. Arsh, N. Kar, S. Das, and S. Deb, "Multiple Approaches Towards Authentication Using Keystroke Dynamics", International Conference on Machine Learning and Data Engineering (ICMLDE 2023), Procedia Computer Science 235 (2024), pp. 2609 2618.

[25] O. Alpar, "Biometric Touchstroke Authentication by Fuzzy Proximity of Touch Locations", Future Generation Computer Systems, Vol. 86, Sept. 2018, pp. 71 - 80.

[26] Anaya and S. Singh, "Keystroke Dynamics for Continuous Authentication", 2018 8th International Conference on Cloud Computing, Data Science Engineering (Confluence), Noida.

[27] S. Singh, A. Inamdar, A. Kore, and A. Pawar, "Analysis of Algorithms for User Authentication using Keystroke Dynamics", 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai.

[28] A. Negi, S. Rathore, and D. Sadhya, "USB Keypress Injection Attack Detection via Free-Text Keystroke Dynamics", 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN), Noida,.

[29] D. Senarath, S. Tharinda, M. Vishvajith, S. Rasnayaka, S. Wickramanayake, and D. Meedeniya, "Re-evaluating Keystroke Dynamics for Continuous Authentication", 2023 3rd International Conference on Advanced Research in Computing (ICARC), Srilanka.

[30] C. Lin, J. He, C. Shen, Q. Li, and Q. Wang, "CrossBehaAuth: Cross-Scenario Behavioral Biometrics Authentication Using Keystroke Dynamics", IEEE Transactions on Dependable and Secure Computing, Vol. 20, No: 3, 2023, pp. 2314 - 2327.

[31] B. Ayotte, M. Banavar, D. Hou, and S. Schuckers, "Fast Free-Text Authentication via Instance-Based Keystroke Dynamics", IEEE Transactions on Biometrics, Behavior, and Identity Science, Vol: 2, No: 4, 2020, pp. 377 - 387.